

PHNL030926

PCT/IB2004/051226

CLAIMS:

1. A method of generating an Authorized Domain (AD), the method comprising the steps of

- selecting a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (100),
- binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID), and
- binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID), and thereby obtaining a number of devices (D1, D2, ..., DM) and a number of persons (P1, P2, ..., PN₁) that is authorized to access a content item of said Authorized Domain (100).

2. A method according to claim 1, characterized in that the method further comprises the step of:

- binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD) given by the domain identifier (Domain_ID).

3. A method according to claims 1 – 2, characterized in that the step of binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID) comprises:

- obtaining or generating a Domain Users List (DUC) comprising the domain identifier (Domain_ID) and a unique identifier (Pers_ID1, Pers_ID2, ..., Pers_IDN₁) for a user (P1, P2, ..., PN₁) thereby defining that the user is bound to the Authorized Domain (100),

and/or in that

- the step of binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID) comprises:
 - obtaining or generating a Domain Devices List (DDC) comprising the domain identifier (Domain_ID) and a unique identifier (Dev.ID1, Dev.ID2, ..., Dev.IDM) for a device (D1, D2, ..., DM) thereby defining that the device is bound to the domain (100).

PHNL030926

PCT/IB2004/051226

4. A method according to claims 2 – 3, characterized in that the step of binding at least one content item (C₁, C₂, ..., C_{N₂}) to the Authorized Domain (AD) comprises:

- binding a content item (C₁, C₂, ..., C_{N₂}) to a User Right (URC₁, URC₂, ... URC_{N₂}), where said User Right (URC₁, URC₂, ... URC_{N₂}) is bound to a user (P₁, P₂, ..., P_{N₁}) bound to the Authorized Domain (100), and/or
- binding a content item (C₁, C₂, ..., C_{N₂}) to a Device Right (DevRC), where said Device Right (DevRC) is bound to a device (D₁, D₂, ..., D_M) bound to the Authorized Domain (100).

10

5. A method according to claims 2 – 4, characterized in that the step of binding at least one content item (C₁, C₂, ..., C_{N₂}) to the Authorized Domain (100) comprises:

- binding a content item (C₁, C₂, ..., C_{N₃}) to a Domain Right (DRC₁, DRC₂, ... DRC_{N₂}), where said Domain Right (DRC₁, DRC₂, ... DRC_{N₂}) is bound to the Authorized Domain (100).

15

6. A method according to claims 4 or 5, characterized in that the User Right (URC) or the Device Right (DevRC) or the Domain Rights (DRC) comprises rights data (Rights Dat) representing which rights exists in relation to the at least one content item (C₁, C₂, ..., C_{N₂}) bound to the User Right (URC) or the Device Right (DevRC) or the Domain Rights (DRC).

20

7. A method according to any one of the previous claims, characterized in that the method further comprises the step of controlling access to a given content item bound to the Authorized Domain (100) by a given device being operated by a given user, the step comprising:

25

- checking if the given user is bound to the same Authorized Domain (100) as the given content item, or
- checking if the given device is bound to the same Authorized Domain (100) as the given content item,

30 and allowing access for the given user via the given device and/or other devices to the content item if the given user is bound to the same Authorized Domain (100), or allowing access for the given user and/or other users via the given device to the content item if the given device is part of the same Authorized Domain (100).

PHNL030926

PCT/IB2004/051226

8. A method according to any one of claims 1 – 6, characterized in that the method further comprises the step of controlling access to a given content item (C₁, C₂, ..., C_{N₂}), being bound to the Authorized Domain (100) and having a unique content identifier (Cont_ID), by a given device being operated by a given user comprising:
- checking if the Domain Devices List (DDC) of the Authorized Domain (100) comprises an identifier (Dev.ID) of the given device, thereby checking if the given device is bound to the same Authorized Domain (100) as the content item, and/or
 - checking if the Domain User List (DUC) of the Authorized Domain (100) comprises an identifier (Pers_ID) of the given user (P₁, P₂, ..., P_{N₁}) thereby checking if the given user is bound to the same Authorized Domain (100) as the content item,
 - and allowing access to the given content item (C₁, C₂, ..., C_{N₂}) by the given device (D₁, D₂, ..., D_M) for any user if the given device is bound to the same Authorized Domain (100) as the content item being accessed, and/or
 - allowing access to the given content item (C₁, C₂, ..., C_{N₂}) by any device including the given device for the given user if the given user is bound to the same Authorized Domain (100) as the content item being accessed.

9. A method according to claims 7 – 8, characterized in that the step of controlling access of a given content item further comprises:
- checking that the User Right (URC) for the given content item specifies that the given user (P₁, P₂, ..., P_{N₁}) has the right to access the given content item (C₁, C₂, ..., C_{N₂}) and only allowing access to the given content item (C₁, C₂, ..., C_{N₂}) in the affirmative.

- 25 10. A method according to claims 1 – 9, characterized in that every content item is encrypted and that a content right (CR) is bound to each content item and to a User Right (URC) or a Device Rights (DevRC) or a Domain Rights (DRC), and that the content right (CR) of a given content item comprises an decryption key for decrypting the given content item.

- 30 11. A method according to claims 3 - 10, characterized in that
 - the Domain Users List (DUC) is implemented as or included in a Domain Users Certificate, and/or

PHNL030926

PCT/IB2004/051226

22

- the Domain Devices List (DDC) is implemented as or included in a Domain Devices Certificate, and/or
 - the User Right (URC1, URC2, ..., URCN₂) is implemented as or included in a User Right Certificate, and/or
 - 5 - the Device Right (DevRC) is implemented as or included in a Device Right Certificate, and/or
 - the Domain Rights (DRC1, DRC2, ..., DRCN₂) is implemented/included in a Domain Rights Certificate.
- 10 12. A system for generating an Authorized Domain (AD), the system comprising:
 - means for obtaining a domain identifier (Domain_ID) uniquely identifying the Authorized Domain (100),
 - means for binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID), and
 - 15 - means for binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID), and
 - thereby obtaining a number of devices (D1, D2, ..., DM) and a number of persons (P1, P2, ..., PN₁) that is authorized to access a content item of said Authorized Domain (100).
- 20 13. A system according to claim 1, characterized in that the system further comprises:
 - means for binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD) given by the domain identifier (Domain_ID).
- 25 14. A system according to claims 12 – 13, characterized in that the means for binding at least one user (P1, P2, ..., PN₁) to the domain identifier (Domain_ID) is adapted to:
 - obtain or generate a Domain Users List (DUC) comprising the domain identifier (Domain_ID) and a unique identifier (Pers_ID1, Pers_ID2, ..., Pers_IDN₁) for a user (P1, P2, ..., PN₁) thereby defining that the user is bound to the Authorized Domain (100),
- 30 and/or in that

PHNL030926

PCT/IB2004/051226

the means for binding at least one device (D1, D2, ..., DM) to the domain identifier (Domain_ID) is adapted to:

- obtain or generate a Domain Devices List (DDC) comprising the domain identifier (Domain_ID) and a unique identifier (Dev.ID1, Dev.ID2, ..., Dev.IDM) for a device (D1, D2, ..., DM) thereby defining that the device is bound to the domain (100).

15. A system according to claims 13 – 14, characterized in that the means for binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (AD) is adapted to:

- bind a content item (C1, C2, ..., CN₂) to a User Right (URC1, URC2, ... URCN₂), where said User Right (URC1, URC2, ... URCN₂) is bound to a user (P1, P2, ..., PN₁) bound to the Authorized Domain (100), and/or
- bind a content item (C1, C2, ..., CN₂) to a Device Right (DevRC), where said Device Right (DevRC) is bound to a device (D1, D2, ..., DM) bound to the Authorized Domain (100).

16. A system according to claims 13 – 15, characterized in that the means for binding at least one content item (C1, C2, ..., CN₂) to the Authorized Domain (100) is adapted to:

- bind a content item (C1, C2, ..., CN₃) to a Domain Right (DRC1, DRC2, ... DRCN₂), where said Domain Right (DRC1, DRC2, ... DRCN₂) is bound to the Authorized Domain (100).

17. A system according to claims 15 or 16, characterized in that the User Right (URC) or the Device Right (DevRC) or the Domain Rights (DRC) comprises rights data (Rights Dat) representing which rights exists in relation to the at least one content item (C1, C2, ..., CN₂) bound to the User Right (URC) or the Device Right (DevRC) or the Domain Rights (DRC).

30 18. A system according to claims 12 – 17, characterized in that the system further comprises means for controlling access to a given content item bound to the Authorized Domain (100) by a given device being operated by a given user, where the means is adapted to:

PHNL030926

PCT/IB2004/051226

24

- check if the given user is bound to the same Authorized Domain (100) as the given content item, or
 - check if the given device is bound to the same Authorized Domain (100) as the given content item,
- 5 and allow access for the given user via the given device and/or other devices to the content item if the given user is bound to the same Authorized Domain (100),
or allow access for the given user and/or other users via the given device to the content item if the given device is part of the same Authorized Domain (100).

10 19. A system according to any one of claims 12 – 17, characterized in that the system further comprises means for controlling access to a given content item (C1, C2, ..., CN₂), being bound to the Authorized Domain (100) and having a unique content identifier (Cont_ID), by a given device being operated by a given user, where the means is adapted to:

- check if the Domain Devices List (DDC) of the Authorized Domain (100) comprises an identifier (Dev.ID) of the given device, thereby checking if the given device is bound to the same Authorized Domain (100) as the content item, and/or
- check if the Domain User List (DUC) of the Authorized Domain (100) comprises an identifier (Pers_ID) of the given user (P1, P2, ..., PN₁) thereby checking if the given user is bound to the same Authorized Domain (100) as the content item,
- 15 - and allow access to the given content item (C1, C2, ..., CN₂) by the given device (D1, D2, ..., DM) for any user if the given device is bound to the same Authorized Domain (100) as the content item being accessed, and/or
- allow access to the given content item (C1, C2, ..., CN₂) by any device including the given device for the given user if the given user is bound to the same Authorized 20 Domain (100) as the content item being accessed.

- 25 20. A system according to claims 18 – 19, characterized in that the means for controlling access of a given content item is further adapted to further:
- check that the User Right (URC) for the given content item specifies that the given user (P1, P2, ..., PN₁) has the right to access the given content item (C1, C2, ..., CN₂) and only allowing access to the given content item (C1, C2, ..., CN₂) in the affirmative.

PHNL030926

PCT/IB2004/051226

25

21. A system according to claims 12 – 20, characterized in that every content item is encrypted and that a content right (CR) is bound to each content item and to a User Right (URC) or a Device Rights (DevRC) or a Domain Rights (DRC), and that the content right (CR) of a given content item comprises an decryption key for decrypting the given content

5 item.

22. A system according to claims 24 - 21, characterized in that

- the Domain Users List (DUC) is implemented as or included in a Domain Users Certificate, and/or
- 10 - the Domain Devices List (DDC) is implemented as or included in a Domain Devices Certificate, and/or
- the User Right (URC₁, URC₂, ..., URC_{N₂}) is implemented as or included in a User Right Certificate, and/or
- the Device Right (DevRC) is implemented as or included in a Device Right Certificate, and/or
- 15 - the Domain Rights (DRC₁, DRC₂, ..., DRC_{N₂}) is implemented/included in a Domain Rights Certificate.

23. A computer readable medium having stored thereon instructions for causing 20 one or more processing units to execute the method according to any one of claims 1 – 11.